UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,428	04/05/2006	Olivier Brique	90500-000035/US	2506

30593 7590 05/28/2008

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
05/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/517,428	BRIQUE ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/10/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the original filing of April 5, 2006. Claims (17-35) are pending and have been considered below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 17- 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Bar-On (US Patent No. 7,031,470).

3. As to claim 17, Bar-On teaches **a data exchange method between two devices locally connected to one another, especially between a security module and a receiver, the first device** (i.e., player security chip) **comprising at least one first encrypting key of a pair of asymmetric keys and the second device** (i.e., disk security chip) **comprising at least the second encrypting key of said pair of asymmetric keys, these keys being previously initialised in the first and second device, this method comprising:**

generating, at least one first random number in the first device (i.e., Bar-On teaches a player security chip sending a random number R to disk security chip [col. 5, lines 50-55]),

generating, at least one second random number in the second device (i.e., Bar-On teaches the disk security chip sending the player security chip an encrypted concatenation of a hash function of R [col. 5, lines 50-55]),

encrypting said first random number by said first encrypting key (i.e., Bar-on teaches encrypting the concatenation of a hash function of R with a disk key [col. 5, lines 55-56],

encrypting said second random number by said second encrypting key (i.e., Bar-On teaches the disk security chip sending the player security chip an encrypted concatenation of a hash function of R [col. 5, lines 50-55]),

transmitting said first encrypted random number to the second device (i.e., Bar-On teaches a player security chip sending a random number R to disk security chip [col. 5, lines 50-55]),

transmitting said second encrypted random number to the first device (i.e., Bar-On teaches the disk security chip sending the player security chip an encrypted concatenation of a hash function of R [col. 5, lines 50-55]),

decrypting the first encrypted random number in said second device (i.e., Bar-On teaches computing a hash of random number R and content key for which was encrypted with the disk key [col. 5, lines 55-66],

decrypting the second encrypted random number in said first device (i.e., Bar-On teaches decrypting concatenation [col. 5, lines 55-60]),

combining said random numbers generated by one of the devices and received by the other device to generate a session key (i.e., content key) (i.e., Bar-On teaches obtaining the content key from the concatenation [col. 5, lines 60-65]),

and using the session key (i.e., content key) **to encrypt and decrypt all or part of the exchanged data between the first and second device** (i.e., Bar-On teaches using the content key to decrypt control words [col. 5, lines 60-65]).

4. As to claim 18, Bar-On teaches **a data exchange method where random number, generated by the first device and decrypted by the second device is encrypted by said second device by means of said second encrypting key** (i.e., player security chip sends a random number to disk security chip and the disk security chip sends encrypted concatenation to player chip [col. 5, lines 50-58], **is transmitted in a encrypted form to said first device** (i.e., Bar-On teaches sending a encrypted concatenation [col. 5, lines 53-57]), **is decrypted in this first device by means of the first encrypting key** (i.e., disk key) **and is compared to said random number generated by the first device** (i.e., Bar-On teaches decrypting the concatenation and computing the hash and performing a comparison [col. 5, lines 55-60]), **and where the data transfer is stopped if the compared random numbers are not identical** [e.g., correct] (i.e., Bar-On teaches computing the hash and comparing random the numbers [col. 5, lines 57-62]).

5. As to claim 19, Bar-On teaches **a data exchange method where the random number, generated by the second device and decrypted by the first device is**

encrypted by said first device by means of said first encrypting key is transmitted in a encrypted form to said second device (col. 10, lines 49 -52), **is decrypted in this second device by means of the second encrypting key and is compared to said random number generated by the second device** (col. 10, lines 59-61), **and wherein the data transfer is stopped if the compared random numbers are not identical** (col. 10, lines 61-67).

6. As to claim 20, Bar-On teaches **a Data exchange method in which said first device and said second device contain a symmetric encrypting key** (i.e., disk key), **where the random numbers** (i.e., random number R) **are combined** (i.e., concatenation) **with said symmetric key** (i.e., disk key) to generate (i.e., hash function to obtain content key from concatenation) **a session key** (i.e., content key) (col. 5, lines 54-56 and lines 60-61).

7. As to claim 21, Bar-On teaches **a data exchange method where the combination of said random numbers** (e.g., random number R) **is a concatenation** (i.e., Bar-On teaches a concatenation hash function of random number R [col. 5, lines 54-56]).

8. As to claim 22, Bar-On teaches a **data exchange method where the combination of said random numbers** (e.g., random number R) **is a concatenation** (i.e., Bar-On teaches a concatenation hash function of random number R [col. 5, lines 54-56]).

9. As to claim 23, Bar-On teaches **a data exchange method where the session key** (i.e., content key) **is regenerated** (i.e., computing the hash) **in function of a determined parameter of use** (i.e., session key used to decrypt control word) [col. 5, lines 58-64].

10. As to claim 24, Bar-On teaches **a data exchange method the determined parameter of use is the duration of use** (i.e., control word) (i.e., one of ordinary skill in the art recognizes the control word ability of control use [col. 5, lines 58-64]).

11. As to claim 25, Bar-On teaches **a data exchange method where at least one of the two devices measures at least one representative physical parameter** (i.e. opacity) **of the communication, such as the line impedance and/or the electric consumption** (i.e., voltage)**, where one compares the values measured to the reference values** [e.g., controlling voltage]**, and where one acts on the data exchange** (i.e., communicate the desire information from the disk chip) **when the measured parameters differ from the reference values more than a threshold value** [e.g., controlling voltage] (i.e., Bar-On teaches as an alternative to the radio communication described above, it is possible to optically provide contactless power supply and communication between disk chip 16 and player chip 18. Bar-On teaches as an example, power can be supplied by a light source which directs light to a photovoltaic cell. Bar-On teaches communication to disk chip 16 can be achieved by illuminating selected tracks on disk 12 that are covered with photo-sensitive materials,

whereby disk chip 16 monitors the tracks that are illuminated by the laser head. Bar-On teaches communication from disk chip 16 can be accomplished by covering the laser-head illumination tracks on the disk with voltage-controlled semi-opaque materials, such as liquid crystals, located upon a reflective material. Bar-On teaches a disk chip 16 can then control the opacity of the semi-opaque material by appropriately controlling the voltage, the degree of opacity being used to communicate the desired information from disk chip 16 to player chip 18 [col. 9, lines 5-25]).

12. As to claim 26, Bar-On teaches **a data exchange method where one acts by stopping the data exchange between the two devices** (i.e., Bar-On teaches permitting the commencement of a particular action on the basis of successful a verification [col. 11, lines 1-5]. One of ordinary skill in the art would recognize the ability to permit commencement of a particular action upon successful verification inherently suggest the ability to cease a particular action due unsuccessful verification).

13. As to claim 27, Bar-On teaches **a data exchange method where the session key** (e.g., content key) **is regenerated in function of a determined parameter of use and wherein the determined parameter of use is the representative physical parameter** (i.e., noisy diode) **of the Communication** (i.e., Bar-On teaches a noisy diode use to generate the random number for which the random number is used in the hash function [col. 10, lines 42-67]. Bar-On teaches the hash function is used to generate the content key (i.e., session key) [col. 5, lines 54-64]).

14. As to claim 28, Bar-On teaches a **data exchange method where at least one of the devices generates at least one supplementary random number** (col. 10, lines 42-45), **this supplementary random number is encrypted by said first encrypting key** (i.e., disk key) , **this supplementary encrypted random number is transmitted to the second device** (col. 5, lines 50-55), **this transmitted encrypted supplementary random number** (i.e. random number R) **is decrypted in this second device** (col. 5, lines 50-55), **the decrypted supplementary random number is encrypted by said second encrypting key** (col. 5, lines 52-57), **the supplementary encrypted random number is transmitted to the first device** (col. 10, lines 49-53), **the supplementary random number decrypted in the first device is compared to the initial supplementary random number generated in said first device** (col. 10, lines 59-65), **the information exchange is interrupted if the comparison indicates that the two compared numbers are not identical** (col. 10, lines 60-65).

15. As to claim 29, Bar-On teaches **a data exchange method where at least one of the devices determines at least one predefined fixed number** (i.e., random number) **memorized** (i.e., stored) **in the two devices** (i.e., Bar-On teaches generating a random number R and stored [col. 10, liens 34-37]), **this predefined fixed number** (i.e., random number) **is encrypted by said first encrypting key** (i.e., Bar-On teaches encrypting the random number [col. 10, lines 50-55]) , **this predefined fixed encrypted number is transmitted to the second device** (i.e., Bar-On teaches sending encrypted random number [col. 10, lines 49-53]), **this transmitted encrypted predefined fixed number is decrypted in this second device** (i.e., ...decrypting [col. 5, lines 52-57[),

the predefined fixed number decrypted in the second device is compared to the predefined fixed number memorized in this second device (i.e., … comparison [col. 10, lines 59-65]), **the data exchange is interrupted if the comparison indicates that the two compared numbers are not identical** (i.e. Bar-On teaches comparing for equivalency) (i.e., Bar-On teaches permitting the commencement of a particular action on the basis of successful a verification [col. 11, lines 1-5]. One of ordinary skill in the art would recognize the ability to permit commencement of a particular action upon successful verification inherently suggest the ability to cease a particular action due unsuccessful verification).

16. As to claim 30, Bar-On teaches a **data exchange method where each of the numbers** (i.e., random numbers) **is encrypted separately** (i.e., Bar-On teaches each random number generated is different. Bar-On further teaches the encryption of each of the random numbers is different [col. 10, lines 50-55]).

17. As to claim 31, Bar-On teaches a **data exchange method according where each of the numbers** (i.e., random numbers) **is encrypted separately** (i.e., Bar-On teaches each random number generated is different. Bar-On further teaches the encryption of each of the random numbers is different [col. 10, lines 50-55]).

18. As to claim 32, Bar-On teaches a **data exchange method where a combination of each of the numbers is encrypted** (i.e., Bar-On teaches different encryption based on different numbers [col. 10, lines 50-55]).

19. As to claim 33, Bar-On teaches a **data exchange method where a combination of each of the numbers is encrypted** (i.e., Bar-On teaches different encryption based on different numbers [col. 10, lines 50-55]).

20. As to claim 34, Bar-On teaches **a receiver for carrying out the method this receiver comprising at least one calculation unit** (i.e., player security chip computing hash/ [col. 5, lines 55-60])**, a read-only memory** [col. 9, lines 40-45], **a demultiplexer** [17, fig. 1], **a descrambler** [15, fig, 1], **a digital/analog converter** (i.e., descrambler in conjunction with decoder [col. 7, lines 40-47])**, an external memory** (i.e., system CPU fig. 1) **and a sound and image descrambler** [15, fig, 1], **where at least the calculation unit** (i.e., player security chip computing hash/ [col. 5, lines 55-60]), **the read-only memory and the descrambler are contained in a same electronic chip and wherein at least one of the encrypting keys is stored in said electronic chip** (i.e., Bar-On teaches a disk key programmed in a disk chip [col. 9, lines 53-56]).

21. As to claim 35, Bar-On teaches **a receiver where at least one of the numbers is stored in said electronic chip** (i.e., Bar-On teaches a random number stored on a player chip [col. 10, liens 34-37]).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/

Examiner, Art Unit 2131

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131